

# CIPHERING COMMUNICATION SYSTEM

Publication number: JP6112936

Publication date: 1994-04-22

Inventor: KOYAIZU IKURO

Applicant: NIPPON TELEGRAPH & TELEPHONE

Classification:

- international: G09C1/00; H04L9/06; H04L9/08; H04L9/14;  
H04L12/02; G09C1/00; H04L9/06; H04L9/08;  
H04L9/14; H04L12/02; (IPC1-7): H04L9/06; G09C1/00;  
H04L9/14; H04L12/02

- european:

Application number: JP19920262345 19920930

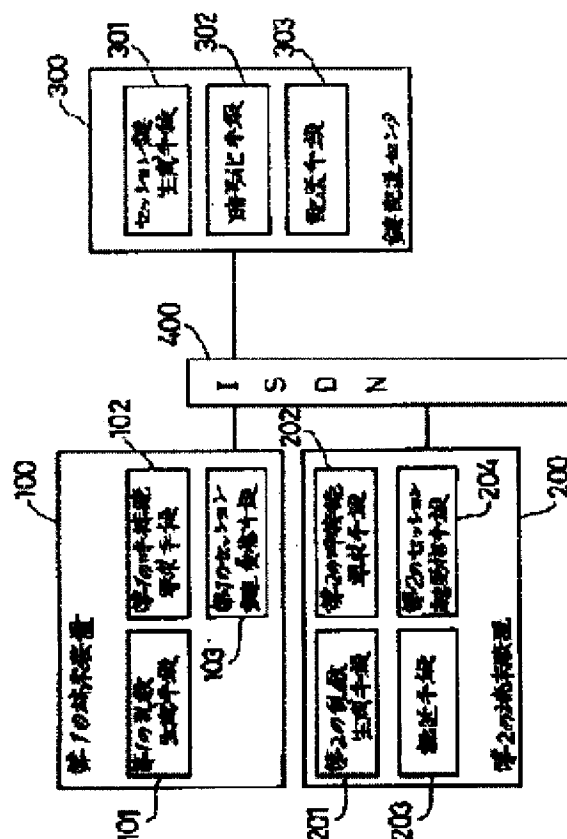
Priority number(s): JP19920262345 19920930

Report a data error here

## Abstract of JP6112936

**PURPOSE:** To provide a ciphering communication system of the common key system not requiring complicated key management in which a communication charge of center access is less expensive.

**CONSTITUTION:** The system is provided with a 1st terminal equipment 100 including a 1st random number generating means 101, a 1st call connection request means 102, and a 1st session key reception means 103, with a 2nd terminal equipment 200 including a 2nd random number generating means 201, a 2nd call connection request means 202, a 2nd session key reception means 204, and a transfer means 203, and with a key delivery center 300 including a session key generating means 301, a ciphering means 302, and a delivery means 303 adding a ciphered signal by the ciphering means 302 to a call number release request message and delivering the result.



(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平6-112936

(43)公開日 平成6年(1994)4月22日

(51)IntCl. <sup>5</sup>	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/06				
9/14				
G 0 9 C 1/00		8837-5L		
		7117-5K	H 0 4 L 9/ 02	Z
		8732-5K	11/ 02	Z

審査請求 未請求 請求項の数 2 (全 10 頁) 最終頁に続く

(21)出願番号 特願平4-262345

(22)出願日 平成4年(1992)9月30日

(71)出願人 000004226

日本電信電話株式会社

東京都千代田区内幸町一丁目1番6号

(72)発明者 小柳津 育郎

東京都千代田区内幸町1丁目1番6号 日

本電信電話株式会社内

(74)代理人 弁理士 伊東 忠彦

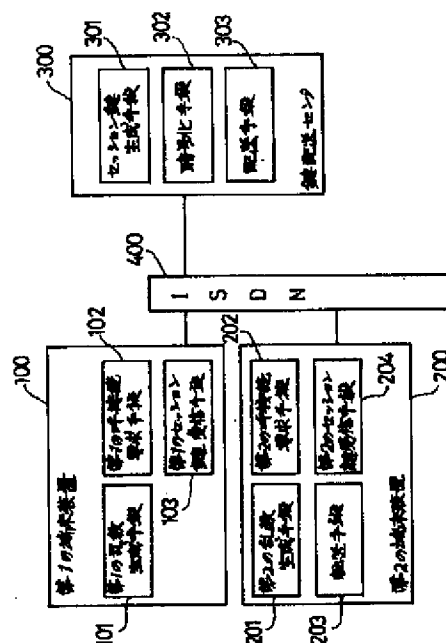
(54)【発明の名称】 秘話通信システム

(57)【要約】

【目的】 本発明の目的は、センタアクセスの通信料が安価で且つ複雑な鍵管理を必要としない共通鍵方式の秘話通信システムを提供することである。

【構成】 本発明は、第1の乱数生成手段101と、第1の呼接続要求手段102と、第1のセッション鍵受信手段103を含む第1の端末装置100と、第2の乱数生成手段201と、第2の呼接続要求手段202と、第2のセッション鍵受信手段204と、転送手段203を含む第2の端末装置200と、セッション鍵生成手段301と、暗号化手段302と、暗号化手段302により暗号化されたものを呼番号解放要求メッセージに付加して配送する配送手段303を含む鍵配送センタ300を有する。

本発明の原理構成図



## 【特許請求の範囲】

【請求項1】 I S D N回線に接続される複数の端末装置と鍵配送センタからなり、鍵配送センタから配送されるセッション鍵を用いて暗号通信を行う通信システムにおいて、

第1の乱数を生成する第1の乱数生成手段と、呼設定要求メッセージに自加入者番号と該第1の乱数とを付加して通信相手となる端末装置に呼接続要求する第1の呼接続要求手段と、応答メッセージに付加された前記セッション鍵を受信する第1のセッション鍵受信手段を含む第1の端末装置と、

第2の乱数を生成する第2の乱数生成手段と、呼設定要求メッセージに自加入者番号と該第2の乱数及び前記第1の端末装置の加入者番号と前記第1の乱数を付加して鍵配送センタに呼接続要求する第2の呼接続要求手段と、前記鍵配送センタからの呼解放要求メッセージに付加されたセッション鍵を受信する第2のセッション鍵受信手段と、前記鍵配送センタからの前記セッション鍵を応答メッセージに付加して前記第1の端末装置に転送する転送手段を含む第2の端末装置と、前記第2の端末装置からの呼設定要求メッセージの第1の端末装置の加入者番号と前記第2の端末装置の加入者番号が登録されている場合にはセッション鍵を生成するセッション鍵生成手段と、該セッション鍵生成手段により生成したセッション鍵と、前記第1の乱数を前記第1の端末装置の暗号鍵で暗号化し、該セッション鍵と前記第2の乱数を前記第2の端末装置の暗号鍵で暗号化する暗号化手段と、該暗号化手段により暗号化されたものを呼番号解放要求メッセージに付加して配送する配送手段を含む鍵配送センタを有することを特徴とする秘話通信システム。

【請求項2】 前記鍵配送センタに登録されている端末装置の暗号鍵に、暗号鍵を前記鍵配送センタの秘密鍵と秘密パラメータとから生成する暗号鍵生成手段を含む鍵配送センタを有する請求項1記載の秘話通信システム。

## 【発明の詳細な説明】

## 【0001】

【産業上の利用分野】本発明は、共通鍵暗号アルゴリズムを用いてI S D N回線に接続した端末装置間で暗号通信を行う場合の秘話通信システムに係り、特に事業所等の複数メンバからなるグループ内で、共通鍵方式の暗号通信を行う場合に好適な秘話通信システムに関する。

## 【0002】

【従来の技術】共通鍵暗号アルゴリズムは、暗号文を作成するときの鍵（暗号鍵）と、暗号文を元に戻すときの鍵（復号鍵）に同じ数値データを用いる暗号方式である。この暗号方式を用いて各端末装置が互いに他と秘密の通信を行うには、各端末装置毎に、互いに通信する端末装置数に等しい暗号鍵が必要である。しかしながら、端末装置数が増えれば鍵の数が膨大となる。

【0003】このため、従来、各端末装置が秘密にする暗号鍵を登録しておく鍵配送センタを別に設置し、端末装置# iが端末装置# jと暗号通信を開始する度に鍵配送センタにアクセスして登録してある暗号鍵 $K_i$ 、 $K_j$ で暗号化したセッション鍵を配送して貰う。端末装置# iと端末装置# jは、暗号化されたセッション鍵を互いに復号し、このセッション鍵を用いて以後の通信を暗号化するのが一般的である。

## 【0004】

【発明が解決しようとする課題】従来の技術のような鍵配送センタがセッション鍵を配送する方式は、端末装置が管理する鍵は一つでよい。しかし、この方法の第1の問題として、実際の通信に先立って鍵配送センタからセッション鍵を受け取るための通信料が別に必要である。

【0005】また、第2の問題として、鍵配送センタに端末装置の鍵ファイルが必要であり、第3者がそのファイルへの不法アクセスを防止するために膨大な鍵ファイルを保護された領域に置く必要がある。このため、多数の端末装置を接続し、鍵の書き換えを行う場合などには複雑な鍵管理を行う必要がある。

【0006】本発明は上記の点に鑑みてなされたもので、センタアクセスの通信料が安価で且つ複雑な鍵管理を必要としない共通鍵方式の秘話通信システムを提供することを目的とする。

## 【0007】

【課題を解決するための手段】図1は、本発明の原理構成図である。

【0008】本発明は、I S D N回線400に接続される複数の端末装置と鍵配送センタ300からなり、鍵配送センタ300から配送されるセッション鍵を用いて暗号通信を行う通信システムにおいて、第1の乱数を生成する第1の乱数生成手段101と、呼設定要求メッセージに自加入者番号と第1の乱数とを付加して通信相手となる端末装置に呼接続要求する第1の呼接続要求手段102と、応答メッセージに付加されたセッション鍵を受信する第1のセッション鍵受信手段103を含む第1の端末装置100と、第2の乱数を生成する第2の乱数生成手段201と、呼設定要求メッセージに自加入者番号と第2の乱数及び第1の端末装置100の加入者番号と第1の乱数を付加して鍵配送センタ300に呼接続要求する第2の呼接続要求手段202と、鍵配送センタ300からの呼解放要求メッセージに付加されたセッション鍵を受信する第2のセッション鍵受信手段204と、鍵配送センタ300からのセッション鍵を応答メッセージに付加して第1の端末装置100に転送する転送手段203を含む第2の端末装置200と、第2の端末装置200からの呼設定要求メッセージの第1の端末装置100の加入者番号と第2の端末装置200の加入者番号が登録されている場合にはセッション鍵を生成するセッション鍵生成手段301と、セッション鍵生成手段301

により生成したセッション鍵と、第1の乱数を第1の端末装置100の暗号鍵で暗号化し、セッション鍵と第2の乱数を第2の端末装置200の暗号鍵で暗号化する暗号化手段302と、暗号化手段302により暗号化されたものを呼番号解放要求メッセージに付加して配送する配送手段303を含む鍵配送センタ300を有する。

【0009】また、本発明は、鍵配送センタ300に登録されている端末装置に、暗号鍵を鍵配送センタ300の秘密鍵と秘密パラメータとから生成する暗号鍵生成手段を含む。

【0010】

【作用】本発明は、端末装置が秘話通信を行う場合には、呼設定要求メッセージに自加入者番号と乱数を付加して、相手端末装置に呼接続要求を行う。要求された端末装置は、呼接続シーケンスを保留したまま、発信端末装置から送られた加入者番号と乱数に自端末装置の加入者番号と乱数を加えたものを呼設定要求メッセージに付加して、鍵配送センタに呼接続要求する。

【0011】鍵配送センタは、両端末装置が登録されていれば、セッション鍵と両端末装置の暗号鍵を生成し、それぞれの端末装置の暗号鍵で暗号化したセッション鍵と乱数を呼解放要求メッセージに付加して送出する。着信端末装置は、自分と鍵配送センタだけが知る暗号鍵でセッション鍵と自分が生成した乱数を復号し、正しいセッション鍵を受信したことを確認する。次いで、発信端末装置と呼設定シーケンスを再開し、鍵配送センタから受け取った応答メッセージに付加してある暗号化されたセッション鍵と乱数を発信端末装置に転送する。これにより、発信側の端末装置は、鍵配送センタと自分だけが知る暗号鍵を用いて、セッション鍵と最初に送った乱数を復号し、正しいセッション鍵を受信したことを確認することができるため、両端末装置は、受信したセッション鍵を用いて呼設定後の秘話通信を行うことができる。

【0012】

【実施例】以下、図面と共に本発明の実施例を詳細に説明する。

【0013】図2は本発明の一実施例の共通鍵暗号アルゴリズムを用いた秘話通信システムのブロック図を示す。

$$K_i = e K_a (ID_i \parallel G_i \parallel P)$$

但し、 $K_a = K + G_i$

ここで、Kは鍵配送センタ2の秘密鍵、Pは秘密パラメータ（秘密値）を示し、

【数2】

“ $\parallel$ ”

【0020】は連結（concatenation）を示し、“+”はビット対応の排他的論理和を示す。

【0021】図3は、本発明の一実施例の鍵配送センタと端末装置の鍵管理テーブルを示す。同図中、(a)は鍵配送センタの鍵管理テーブルを示し、(b)は端末装

\*【0014】同図において、端末装置1は、ISDN加入者回線のレイヤ1～レイヤ3制御及びレイヤ4から上の上位レイヤのネットワーク制御を行う端末制御部11と暗号演算部12と鍵管理テーブル部13とランダムデータ発生部14から構成されている。

【0015】また、鍵配送センタ2は、ISDN加入者回線のレイヤ1～レイヤ3制御及び上位レイヤの鍵配送制御を行うセンタ制御部21と暗号演算部22と鍵管理テーブル部23及びランダムデータ発生部24から構成されている。暗号演算部11、暗号演算部22については、ブロック暗号であれば、どのような暗号アルゴリズムを採用してもよい。代表的なアルゴリズムとしては、FEAL暗号アルゴリズムやDES暗号アルゴリズムがある。FEAL暗号アルゴリズムの詳細は、文献「宮口他、FEAL-8暗号アルゴリズム、研実報、Vol.37, No.4/5, ページ321～327、1988年」を、DES暗号アルゴリズムの詳細は文献「小山著、情報セキュリティ、電気書院、ページ76～88、1989年刊行」を参照されたい。暗号演算部22は暗号鍵とデータを入力として、平文pを鍵 $K_i$ で暗号化した暗号文 $e K_i(p)$ 、暗号文cを鍵 $K_i$ で復号した平文 $d K_i(c)$ 及びデータdを鍵 $K_i$ で暗号化した結果の最後のブロックの上位4バイトmac( $K_i, d$ )の3種類の演算を実行する。

【0016】〈端末装置設置時の手続〉次に端末装置設置時の手続について説明する。

【0017】端末装置1#iを設置するときには、予め次の手続により、端末装置1#iの鍵管理テーブル部13と鍵配送センタ2の鍵管理テーブル部23の鍵管理テーブルに次の情報を通信とは別の手段により書き込んでおく。

【0018】鍵配送センタ2に端末装置1#iの番号 $ID_i$ と鍵修飾パラメータ $G_i$ を登録する。

【0019】以下に示す式(1)により $F_i$ を生成し、最後の8バイトを端末装置1#iの鍵 $K_i$ とする。端末装置1#iの鍵管理テーブル部13に16バイトの端末装置1#iの加入者番号（公開可能） $ID_i$ 、端末装置1#iの鍵修飾パラメータ（公開可能） $G_i$ と鍵 $K_i$ を書き込む。

【数1】

$$\dots (1)$$

置1#iの鍵管理テーブルを示す。この鍵管理テーブルは、端末装置1と鍵配送センタ2が管理する鍵情報を示すものである。

【0022】同図中(a)及び(b)の $S, S'$ で示される部分は外部からのアクセス禁止の秘密情報を示し、鍵配送センタ2の暗号鍵K及び秘密パラメータP及び端末装置1#iの暗号鍵 $K_i$ は外部からアクセスできない保護された領域に記憶されている。

【0023】次に本発明の一実施例のセッション鍵配送手順について説明する。

5

【0024】図4は本発明の一実施例の呼接続手順を説明するための図を示す。同図(a)はBチャネルを接続し、通話を行う場合を示し、(b)はBチャネルの接続をしない場合を示す。

【0025】ISDN加入者線に接続されたデジタル電話機などの端末装置1#iが通信相手の端末装置1#jを呼び出して回線交換の呼接続を行う手順(以下呼接続手順と記す)は図4(a)のように行われる。即ち、呼接続は発信者1#iからのSETUP(呼設定の要求)メッセージの送出により開始される。ISDN網3からの呼設定処理中の意味をもつCALL PROC (Call Proceeding:呼設定のための処理中の通知)の転送を経て、着信者1#jの呼出が始まると、ALERT (Alerting:着信者を読み出し中の通知)メッセージが発信者1#iに送られる。

【0026】次に着信側端末装置1#jが応答するとCONN (Connect:着信者が応答したことを通知)メッセージが発信端末装置1#iに、CONN ACK (Connect Acknowledge:CONNに対する確認)メッセージがISDN網3から着信端末装置1#jに送られてBチャネルの接続が完了し、通信が始まる(詳細は、例えば文献:「秋山監修、ISDN絵とき読本、頁92~101、オーム社、1988年発行」を参照)。

【0027】また、端末装置1に呼びだされた鍵配送センタ2が呼接続シーケンスの中でセッション鍵を配送するだけで、Bチャネルを接続し、以後のデータ通信を行う必要がない場合は(詳細は後述する)、着呼拒否として、図4(b)のように(a)に示されるALERTおよびCONNメッセージの代わりに、REL COMP (Release Complete:チャネル解放と呼番号解放要求)メッセージで応答して、Bチャネルの接続をすることなく、呼接続手順を終了することができる(詳細は、「日本電信電話(株)、技術参考資料、INSネットワークサービスのインタフェース 第3分冊、電気通信協会、1990年発行」の頁152~頁153、及び頁160~頁161を参照)。

【0028】一方、ISDNには、呼設定時のメッセージに付随して、通信を行うユーザ間で比較的短いデータのやりとりができるユーザ・ユーザ信号(User-to-User Signalling)が付加サービスとして規定されている。

【0029】図5は本発明の一実施例の呼設定要求メッセージの形式を示す。同図(a)は、本付加サービスを利用する場合の呼設定メッセージの形式を示す。共通部41の先頭から個別部42の高位レイヤ整合性までが通常の呼設定時のメッセージで送信される情報であり、ユーザ・ユーザ情報要素が本付加サービスによって転送される情報である。この時、共通部のメッセージタイプは次の表1のメッセージを用いることができる。

【0030】

【表1】

6

SETUP	00000101
ALERT	00000010
CONN	00000111
DISC	01000101
REL	01001101
REL COMP	01011010

各情報要素の詳細及びメッセージタイプに付随する個別部の情報要素の詳細説明は、本発明内容を説明するのに必須ではないので省略するが、詳細は文献:「秋山監修、ISDN絵とき読本、オーム社、1988年発行」、或いは「日本電信電話(株)技術参考資料、ISNネットサービスのインタフェース 第3分冊、電気通信協会、1990年発行」などに詳しく述べられている。

【0031】本発明は、このユーザ・ユーザ信号の付加サービスを利用して鍵配送情報の交換を行う。本発明で使用するユーザ・ユーザ情報要素の形式を図5(b)に示す。ここで、ユーザ・ユーザ情報要素の第1バイトはユーザ・ユーザ情報要素識別子43で01111110、第2バイトは内容長44であり、第3バイト以下のデータバイト長の値を示す。第3バイトはプロトコル識別子45であり、本実施例のようにユーザの必要性に応じて情報内容を構成する場合には、ユーザ特有のプロトコルを表す“00000000”を入れることが決められている(詳細は、文献「日本電信電話(株)技術参考資料、INSネットサービスのインタフェース、第3分冊、電気通信協会、1990年発行」のページ122~123を参照)。第4バイトは、本発明の実施例で定義する表2に示すコマンド46、第5バイトは内容長47で以後の鍵情報の長さを示すバイト数、第6バイト以降に鍵情報48が格納される。

【表2】

コマンド

Q1:暗号化要求	10000000
Q2:暗号化不能	10000001
Q3:暗号化失敗	10000010

なお、図4(b)の“REL COMP”メッセージは網によってDISC (Disconnect:呼解放要求)メッセージに変換されて発信端末装置1#jに解放要求として通知されるが、“REL COMP”メッセージに付加したユーザ・ユーザ情報はDISCメッセージにそのまま付加されて発信端末装置1#iに転送される(詳細は、「日本電信電話(株)、技術参考資料、INSネットサービスのインタフェース第3分冊、電気通信協会、1990年発行」の頁185を参照)。

【0032】〈通信時の手続〉次に、通信時の手続きについて説明する。本実施例では、端末装置1#iが端末装置1#jを呼び出して暗号通信する際の鍵共有手続きを説明する。

【0033】図6は、本発明の一実施例のセッション鍵配送のためのISDN呼接続手順を示す。

【0034】(a) 端末装置1#iはランダムデータ発生部14を起動し、乱数 $R_i$ を生成する。鍵管理テーブル部12から加入者番号 $ID_i$ 、鍵修飾パラメータ $G_i$ を読み出す。次に端末制御部11を起動し、呼設定シーケンスのSETUPメッセージのユーザ・ユーザ情報要素の第2バイトの内容長44を35にセットし、第4バイト以降に暗号化要求コマンドQ1、内容長32、加入者番号 $ID_i$ 、鍵修飾パラメータ $G_i$ 、乱数 $R_i$ を付加して、端末装置1#jに送信する(図6①)。以降の説明では第2バイトの内容長44の記述は省略する。

【0035】(b) 着信端末装置1#jの端末制御部11は、発信端末装置1#iからSETUPメッセージを受信すると、SETUPメッセージのユーザ・ユーザ情報の中身を解析し、暗号化要求コマンドQ1があると、ランダムデータ発生部14を起動し、乱数 $R_j$ を生成する。鍵管理テーブル部12から加入者番号 $ID_j$ 、鍵修飾パラメータ $G_j$ を読み出す。続いて、次のメッセージ\*

$$MAC_1 = \text{mac}(K_i, ID_i \parallel G_i \parallel C_1 \parallel R_i \parallel)$$

$$MAC_2 = \text{mac}(K_j, ID_j \parallel G_j \parallel C_2 \parallel R_j \parallel)$$

である。上記のMAC(Message Authentication Code)は送信者と受信者間で暗号鍵 $K_i$ を共有する場合にだけ同じ結果が得られることから、データdが通信途中で改ざんされていないことを検証するために利用されるコードである。

【0037】次に、センタ制御部21は呼設定シーケンスのREL COMPメッセージのユーザ・ユーザ情報要素を用いて以下のメッセージを端末装置1#jに回答する(図6③)。ユーザ・ユーザ情報要素のメッセージとしては、暗号化要求コマンドQ1、内容長24、鍵 $K_i$ で暗号化した暗号文 $C_1$ 、検証コード $MAC_1$ 、鍵 $K_j$ で暗号化した暗号文 $C_2$ 、検証コード $MAC_2$ である。

$$K_i = dK_j(C_2)$$

$$MAC_2' = \text{mac}(K_i, ID_j \parallel G_j \parallel C_2 \parallel R_j)$$

$MAC_2 = MAC_2'$  ならば、セッション鍵 $K_s$ が正しいと確認し、セッション鍵 $K_s$ を得る。続いて、端末装置1#jは、暗号演算部12にセッション鍵 $K_s$ と手順★

$$MAC_3 = \text{mac}(K_s, ID_i \parallel G_i \parallel R_i)$$

を計算し、CONNメッセージのユーザ・ユーザ情報要素を用いて、鍵配送センタから受信した鍵情報 $|C_1$ 、 $MAC_1$ に付加し、暗号化要求コマンドQ1、内容長16、鍵 $K_i$ で暗号化した暗号文 $C_1$ 、検証コードMA

\*をSETUPメッセージのユーザ・ユーザ情報要素を用いて鍵配送センタ2へ送信する(図6②)。このとき、ユーザ・ユーザ情報要素のメッセージとしては、暗号化要求コマンドQ1、内容長64、加入者番号 $ID_i$ 、鍵修飾パラメータ $G_i$ 、乱数 $R_i$ 、着信端末装置1#jの加入者番号 $ID_j$ 、着信端末1#jの鍵修飾パラメータ $G_j$ 、着信端末1#jの乱数 $R_j$ である。

【0036】(c) 鍵配送センタ2がSETUPメッセージを受信すると、センタ制御部21がSETUPメッセージを解析し、暗号化要求コマンドを検知すると、加入者番号 $ID_i$ 及び鍵修飾パラメータ $G_j$ とから鍵管理テーブル部23を検索し、対応する加入者の鍵修飾パラメータ $G_i$ 及び $G_j$ が登録されているかどうか検査する。受信した鍵修飾パラメータと登録されている鍵修飾パラメータが一致していれば、鍵配送センタ2は、ランダムデータ発生部24を起動して、8バイトのランダムデータを発生させ、セッション鍵 $K_s$ とする。鍵配送センタ2は、暗号演算部22を起動し、前述の式(1)によりセッション鍵 $K_i$ 、 $K_j$ を生成し、 $C_1$ 、 $C_2$ 、検証コード $MAC_1$ 、 $MAC_2$ を計算する。但し、 $C_1 = eK_i(K_s)$ 、 $C_2 = eK_j(K_s)$ 、

【数3】

※【0038】もし、加入者番号 $ID_i$ 、 $ID_j$ のいずれかが登録されていない、あるいは登録されている番号 $ID_i$ と鍵修飾パラメータ $G_i$ が一致しない等の異常が発見された場合は、呼設定シーケンスのREL COMPメッセージのユーザ・ユーザ情報要素を用いてQ2(暗号化不能)メッセージを端末装置1#jに回答する。

【0039】(d) 端末装置1#jは、DISCメッセージを受信し、暗号要求コマンドを検出すると、鍵管理テーブル部13から自己の暗号鍵 $K_j$ を暗号演算部12に与えて、セッション鍵 $K_s$ と検証コード $MAC_2'$ を計算する。

【数4】

★(b)で端末装置1#iから受信した情報 $ID_i$ 、 $G_i$ 及び $R_i$ を与えて、

【数5】

$C_1$ 、検証コード $MAC_3$ のメッセージを端末装置1#iに送信する(図6④)。もし、鍵配送センタ2からQ2(暗号化不能)メッセージを受信するか、または、 $MAC_2 \neq MAC_2'$  ならば、CONNメッセージのユー

ザ・ユーザ情報要素を用いて、Q3メッセージを端末装置1#iに返送し、鍵共有手続きが失敗したことを通知する。なお、セキュリティシステム上失敗の原因はメッセージ内に詳述しない。

【0040】(e) 端末装置1#iはCONNメッセー\*

$$K_i = dK_i(C_i)$$

$$MAC_1' = \text{mac}(K_i, ID_i \parallel G_i \parallel C_i \parallel R_i)$$

【0041】を計算する。また、暗号演算部12に結果のセッション鍵 $K_s$ を与えて、

※

$$MAC_3' = \text{mac}(K_s, ID_i \parallel G_i \parallel R_i)$$

を求める。 $MAC_1 = MAC_1'$  且つ  $MAC_3 = MAC_3'$  ならば、配送されたセッション鍵が鍵配送センタ2から配送されたものであることが証明されるため、端末装置1#jと正しいセッション鍵 $K_s$ を共有したことを確認し、呼接続と鍵共有手続きを完了する。

【0042】端末装置1#iと端末装置1#jは以降のBチャネル暗号通信をセッション鍵 $K_s$ を用いて行う。

【0043】もし、端末装置1#iが暗号化失敗コマンドQ3を受信するか、 $MAC_1 \neq MAC_1'$  か、または、 $MAC_3 \neq MAC_3'$  であると、鍵配送手順の途中で何らかの不都合が生じたことを示しており、安全のため通信を中断する。

【0044】

【発明の効果】暗号通信を行う各端末装置のそれぞれが暗号鍵を鍵配送センタに登録しておき、登録された任意の相手と暗号通信を行う場合に、従来の方法では、端末装置は相手の端末装置との暗号通信に先立って、鍵配送センタに1度回線接続してセッション鍵の配送を行う必要があった。このため、従来の方法では、実データの暗号通信に要する通信料のほかに、鍵配送センタからのセッション鍵を受信するために最低でも1度数分の通信料が別に必要となる問題がある。

【0045】しかしながら、本発明によれば、鍵配送センタと回線接続をせずにセッション鍵の配送を行うため、上記の欠点を解消することができる。また、本発明によれば、鍵配送センタには公開可能な加入者番号と鍵修飾パラメータを登録しておき、鍵配送センタは自己の秘密とする暗号鍵と秘密パラメータから各端末装置の暗号鍵を生成するため、鍵ファイルをもつ必要がなくなる。このため、ただ2つの秘密値を外部からの読み出し禁止にするだけでよい。また、端末装置の移設や、加入者回線を変更した場合には、鍵配送センタの鍵管理テーブルの公開可能な加入者番号または端末装置の鍵修飾パラメータの値を書き換えることによって容易に変更できるため、鍵配送センタの鍵管理が極めて簡単になる。

【図面の簡単な説明】

【図1】本発明の原理構成図である。

\*ジを受信すると、ユーザ。ユーザ情報要素を解析する。暗号要求コマンドQ1があれば、自端末装置のを暗号演算部12に暗号鍵を与えて、

【数6】

※【数7】

【図2】本発明の一実施例の共通鍵暗号アルゴリズムを用いた秘話通信システムのブロック図である。

【図3】本発明の一実施例の鍵配送センタと端末装置の鍵管理テーブルを示す図である。

【図4】本発明の一実施例の呼接続手順を説明するための図である。

【図5】本発明の一実施例の呼設定要求メッセージの形式を示す図である。

【図6】本発明の一実施例のセッション鍵配送のためのISDN呼接続手順を示す図である。

【符号の説明】

1 端末装置

2 鍵配送センタ

3 ISDN網

11 端末制御部

12 暗号演算部

13 鍵管理テーブル

14 ランダムデータ発生部

21 センタ制御部

22 暗号演算部

23 鍵管理テーブル部

24 ランダムデータ発生部

41 共通部

42 個別部

43 ユーザ・ユーザ情報要素識別子

44 内容長

45 ユーザ特有プロトコル

46 コマンド

47 内容長

48 鍵情報

100 第1の端末装置

101 第1の乱数生成手段

102 第1の呼接続要求手段

103 第1のセッション鍵受信手段

200 第2の端末装置

201 第2の乱数生成手段

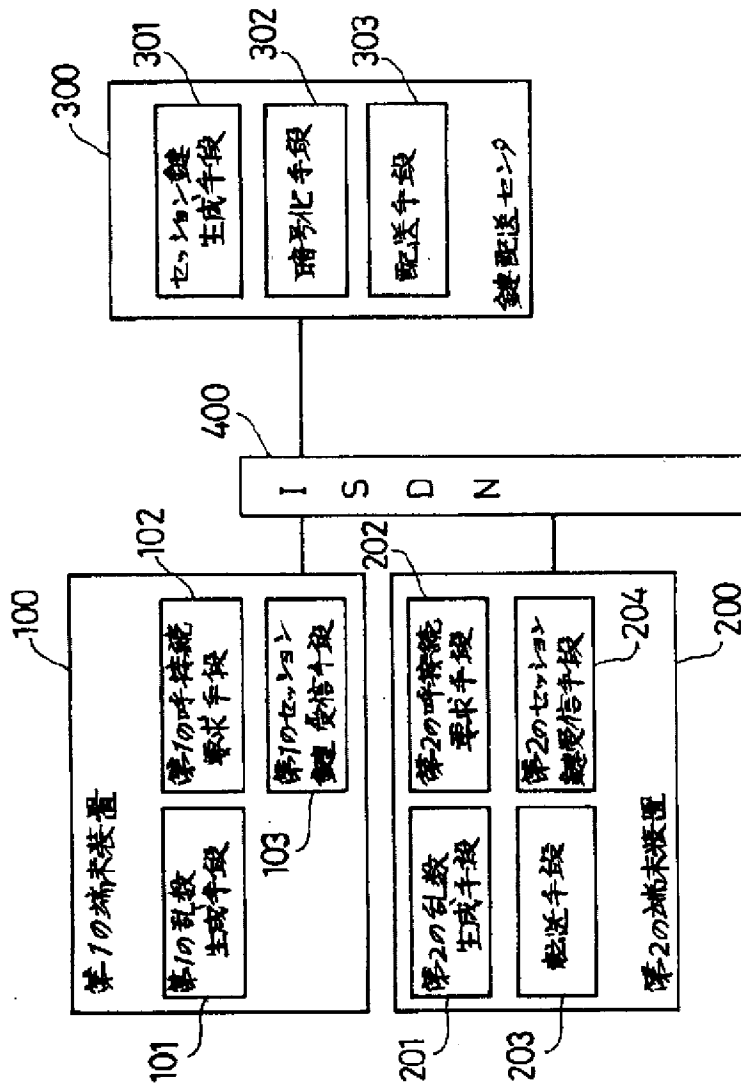
202 第2の呼接続要求手段

203 転送手段  
204 第2のセッション鍵受信手段  
300 鍵配送センタ  
301 セッション鍵生成手段  
302 暗号化手段  
303 配送手段

302 暗号化手段  
303 配送手段  
400 ISDN網

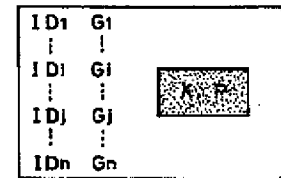
【図1】

## 本発明の原理構成図



【図3】

本発明の一実施例の鍵配送センタと端末装置の鍵管理テーブルを示す図



(a) 鍵配送センタの鍵管理テーブル

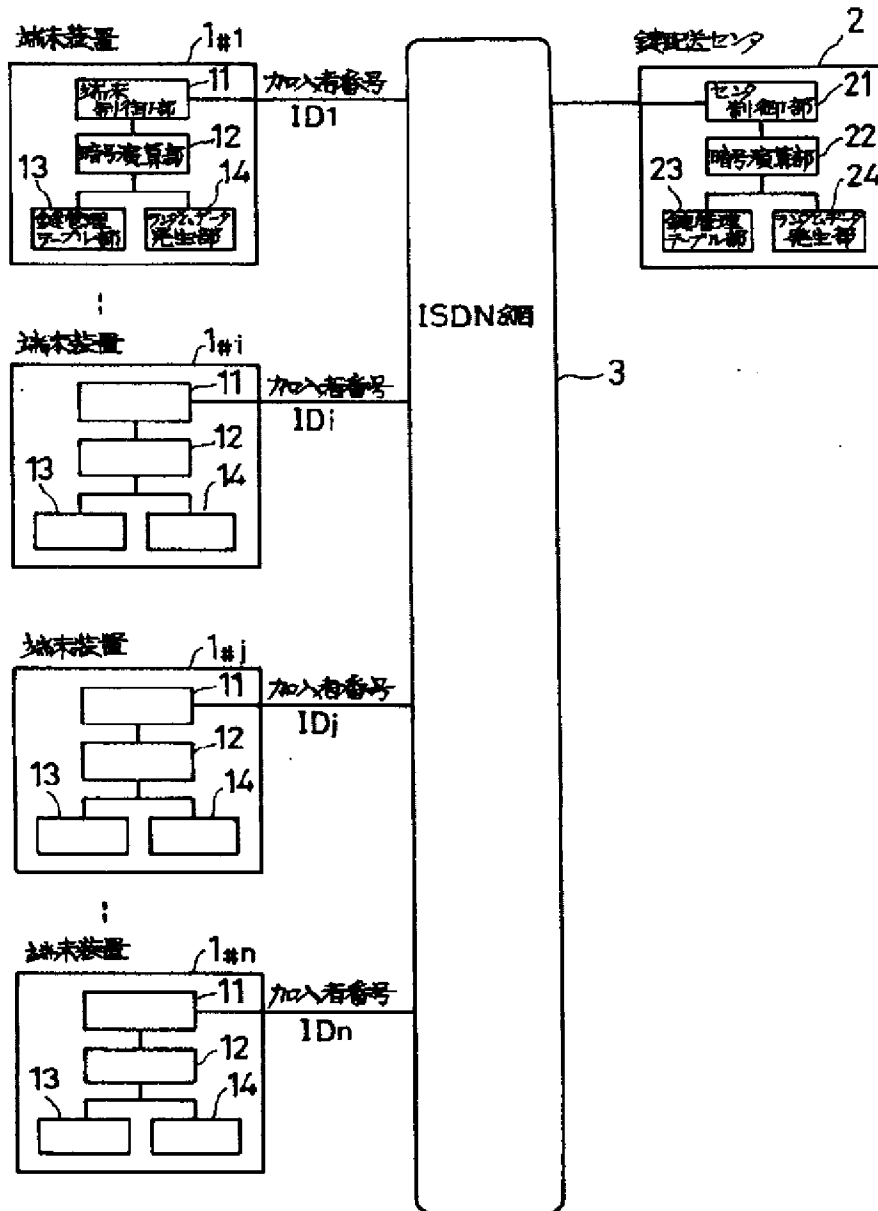
(b) 端末装置*i*の鍵管理テーブル

■: 外部からのアクセス禁止の秘密情報



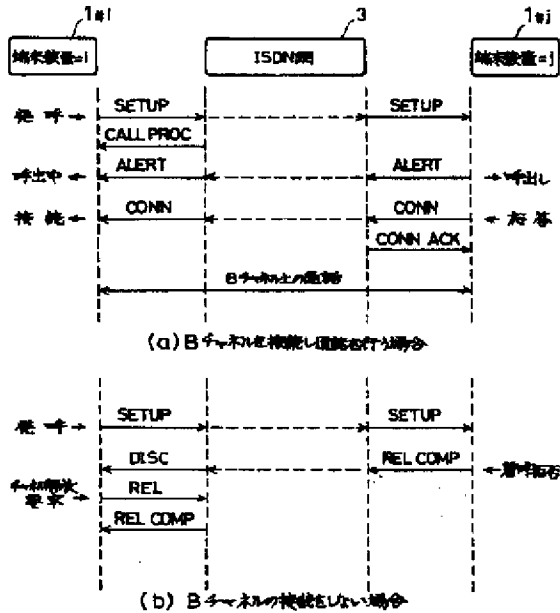
【図2】

本発明の一実施例の共通鍵暗号アルゴリズムを用いた  
秘密通信システムのブロック図



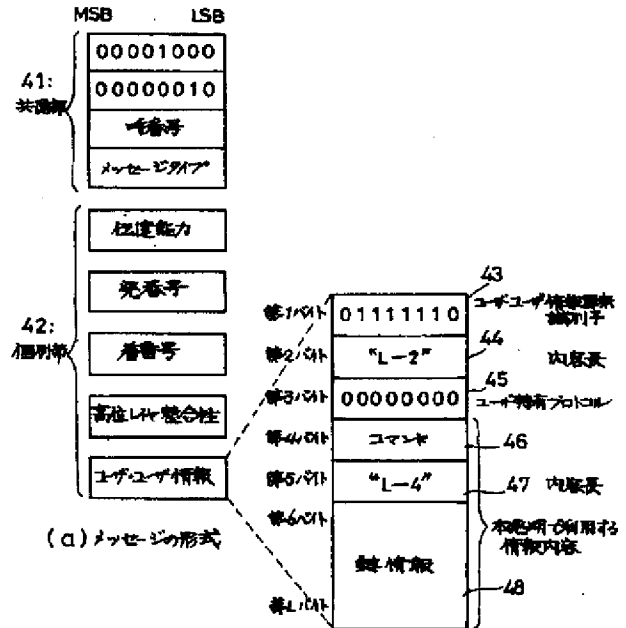
【図4】

本発明の一実施例の呼続統制シーケンスを説明するための図



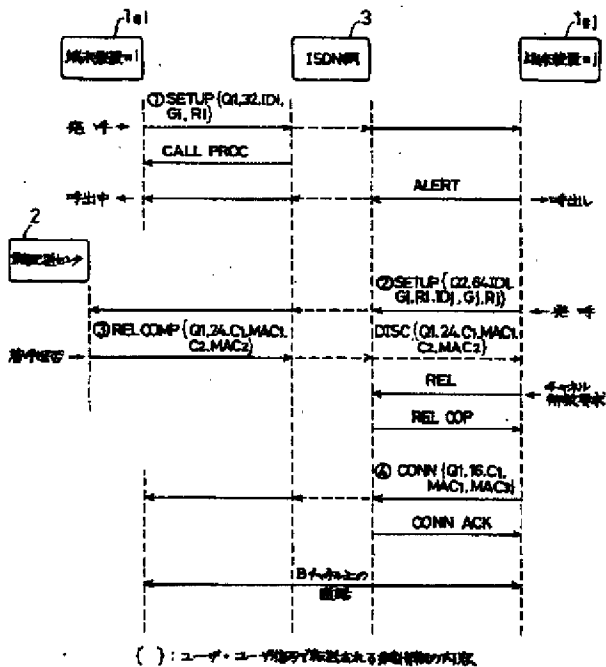
【図5】

呼設定要求メッセージの形式を示す図



【図6】

本発明の一実施例のセッション継送のためISDN呼続統制シーケンスを示す図



フロントページの続き

(51) Int. Cl.<sup>5</sup>  
H 0 4 L 12/02

識別記号

庁内整理番号

F I

技術表示箇所